

IAP9 Rec'd PCT/PTO 30 NOV 2005

DOCKET NO.: 281486US90PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Katsunori MATSUURA

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP05/07254

INTERNATIONAL FILING DATE: April 14, 2005

FOR: ADDRESS CONVERSION METHOD, ACCESS CONTROL METHOD, AND DEVICE
USING THESE METHODS**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION**Commissioner for Patents
Alexandria, Virginia 22313

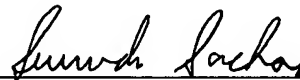
Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2004-118740	14 April 2004
Japan	2004-209367	16 July 2004

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP05/07254.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Masayasu Mori
Attorney of Record
Registration No. 47,301
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application: 2 0 0 4 年 4 月 1 4 日

出 願 番 号

Application Number: 特 願 2 0 0 4 - 1 1 8 7 4 0

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 1 1 8 7 4 0

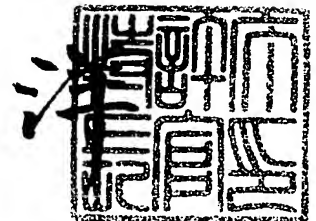
出 願 人

Applicant(s): 日 本 電 信 電 話 株 式 会 社

2 0 0 5 年 5 月 2 0 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【官 告 告】	付 託 願
【整理番号】	NTTH157426
【提出日】	平成16年 4月14日
【あて先】	特許庁長官殿
【国際特許分類】	G06F
【発明者】	
【住所又は居所】	東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
【氏名】	松浦 克智
【特許出願人】	
【識別番号】	000004226
【氏名又は名称】	日本電信電話株式会社
【代理人】	
【識別番号】	100066153
【弁理士】	
【氏名又は名称】	草野 卓
【選任した代理人】	
【識別番号】	100100642
【弁理士】	
【氏名又は名称】	稲垣 稔
【手数料の表示】	
【予納台帳番号】	002897
【納付金額】	16,000円
【提出物件の目録】	
【物件名】	特許請求の範囲 1
【物件名】	明細書 1
【物件名】	図面 1
【物件名】	要約書 1
【包括委任状番号】	9806848

【請求項 1】

ファイアウォール外からのバケットがデータベース部に設定されている通過条件を満たすと、そのバケットをファイアウォール内に通過させるファイアウォール方法であって、上記ファイアウォール外から通過条件設定要求を受信すると、その通過条件設定要求に対する認証処理を行い、

その認証に合格すると、上記通過条件設定要求と対応する通過条件を上記データベース部に設定し、

上記認証処理の前又は上記認証合格後に上記通過条件設定の要求元との安全なセッションを確立してファイアウォール内への通信を可能とし、

上記安全なセッションの切断時に上記設定した通過条件を上記データベース部から削除することを特徴とするファイアウォール方法。

【請求項 2】

上記データベース部に設定する通過条件に、上記通過条件設定要求元のアドレス情報が含まれていることを特徴とする請求項 1 記載のファイアウォール方法。

【請求項 3】

上記安全なセッション確立中はその通信状況を監視して上記安全なセッションにより上記要求元に通知することを特徴とする請求項 1 又は 2 記載のファイアウォール方法。

【請求項 4】

上記通信状況の監視は上記安全なセッションにおけるアクセスに異常が発生するか否かを含み、アクセス異常が発生するとこれを上記通信状況として通知することを特徴とする請求項 2 又は 3 記載のファイアウォール方法。

【請求項 5】

上記認証処理及び上記通過条件設定処理はその要求元の端末が接続されているネットワーク単位で行うことを特徴とする請求項 1 ～ 4 のいずれかに記載のファイアウォール方法。

【請求項 6】

上記安全なセッション確立中にその安全なセッションを通じて新たな接続要求を受信すると、その接続要求の内容を、上記通過条件設定要求を行った要求元に確認させ、

確認が取れると、上記接続要求に対応する通過条件を上記データベース部に追加、又は上記接続要求をファイアウォール内に通過させることを特徴とする請求項 3 ～ 5 のいずれかに記載のファイアウォール方法。

【請求項 7】

ファイアウォール外からのバケットがデータベース部に設定されている通過条件を満たすと、そのバケットをファイアウォール内に通過させるファイアウォール装置であって、

ファイアウォール外から受信された通過条件設定要求に対し認証処理を行う認証処理部と、

上記通過条件設定要求元の端末又はこれが接続されたネットワークとの間に安全なセッションを確立し、その安全なセッションによる通信の終了でその安全なセッションを切断するセッション確立・切断部と、

上記認証処理が合格した上記通過条件設定要求の通過条件を上記データベース部に記録し、切断した安全なセッションと対応する通過条件を上記データベース部から削除する制御部と、

を備えることを特徴とするファイアウォール装置。

【請求項 8】

上記 1 ～ 6 のいずれかに記載した各過程をコンピュータに実行させるためのファイアウォールプログラム。

【請求項 9】

請求項 8 に記載したファイアウォールプログラムが記録されたコンピュータ読み取り可能な記録媒体。

【発明の名称】 ファイアウォール方法、その装置及びプログラム、その記録媒体

【技術分野】

【0001】

この発明はファイアウォール外からのバケットが許可条件を満たすと、そのバケットとファイアウォール内に通過させるファイアウォール、特に許可条件をファイアウォール外から動的に変更することができるようにしたファイアウォール方法、その装置及びプログラム、その記録媒体に関する。

【背景技術】

【0002】

インターネットとローカルエリアネットワーク（LAN）との接続点にファイアウォール装置が挿入され、インターネットからのバケットの宛先や送信元を調べ、設定された安全性規則（セキュリティポリシー）に従って許可されたバケットのみLAN内に通過させ、LAN内の資源を保護することが行われている。

さらに、認証により確認された利用者からのアクセスにより、インターネットからでもファイアウォール装置に設定されているセキュリティポリシーを変更可能にしたものもある（例えば特許文献1参照）。この特許文献1に示す技術を図6を参照して説明する。インターネット11に接続された利用者端末12の利用者が、ファイアウォール装置13内のアクセス制御テーブル13a内のアクセス制御規則を変更したい場合は、利用者端末12から、LAN14に接続されている認証サーバ15に認証依頼をする。認証サーバ15のポート番号はアクセス制御テーブル13aにどのバケットでも通過させる条件として記録されてある。認証依頼には利用者のID（識別情報）と利用者の署名データ、実行したいアクセス内容として自己のIPアドレスやポート番号及びアクセスの相手先のIPアドレスやポート番号が含まれている。

【0003】

認証サーバ15は受信した認証依頼に対する検証を行い、検証に合格すれば、その認証依頼中の「実行したいアクセス内容をアクセス制御テーブル13aに設定するようにファイアウォール装置13に依頼する。従って、この依頼が例えば利用者端末12からLAN14に接続されたウェブ（Web）サーバ16に対するアクセスであれば、利用者は利用者端末12からWebサーバ16にアクセスして例えばコンテンツをダウンロードすることが可能になる。このようにしてファイアウォール外からアクセス制御テーブル13aに設定された実行したいアクセスは所定期間経過した場合又はアクセスが所定期間以上になると元に戻す。

【特許文献1】 特開2003-132020号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかしながら、このような従来のファイアウォール装置においてはセキュリティポリシーを動的に変更できて便利であるが、その認証依頼を行った利用者装置が例えばLAN内のWebサーバからのコンテンツダウンロードを終了した後において、前記通過可能に変更された設定を利用して、不正なバケットがLAN14内に流入してくる恐れがあり、セキュリティを確保することができないという問題があった。

この発明は、この従来の問題を解決するためになされたもので、セキュリティポリシー、つまり通過条件を動的に変えてもセキュリティを確保することのできるファイアウォール方法、その装置及びプログラム、その記録媒体を提供することを目的とする。

【課題を解決するための手段】

【0005】

この発明によればファイアウォール外の利用者端末からアクセス通過条件設定要求を受信すると、その要求に対し認証処理を行い、認証が正常であればその通過条件設定要求に対応する通過条件をデータベースに設定するとともに又は認証処理の前に安全（セキュア

なセッション安全元との間に確立し、前記安全なセッション切斷時にはリーク、ハーベヤの前記通過条件を元に戻す。更に前記安全なセッションを確立中はそのセッションの通信状況をその安全なセッションにより前記要求元に通知するとよい。

【発明の効果】

【0006】

この発明によれば、ファイアウォール外からファイアウォールの通過条件を動的に変更して対応利用者端末からのパケットがファイアウォールを通過できるようにでき、しかもその安全なセッション切斷時にはその通過許可が解除されるため、そのセッション切斷後不正なパケットはファイアウォールを通過できない。更に前述のように確立しているセッションでの通信状況を要求元に通知する場合は、要求元で不正な通信を監視させることができる。

【発明を実施するための最良の形態】

【0007】

以下、この発明の実施の形態について、図面を参照して説明する。

この発明の一実施の形態のファイアウォール装置の機能構成例とこの発明方法の一実施形態のファイアウォール方法の手順例をそれぞれ図1と図2に示す。

この実施の形態のファイアウォール装置21は、インターネットなどの広域通信網(WAN: Wide Area Network)22に接続され、WAN22とのパケットの送受信を行うWANインターフェース部23と、LAN24とのパケットの送受信を行うLANインターフェース部25と、WANインターフェース部23およびLANインターフェース部25が受信したパケットを分析しアクセス制御を行うアクセス制御部26と、アクセス制御部26の要求により利用者(ユーザ)の認証処理を行う認証処理部27と、アクセス制御のためのデータや認証のデータを蓄えているデータベース部28とを備えている。

【0008】

データベース部28の通過条件テーブル28aには、図3Aに示すようなテーブルが記憶されており、アクセス制御部26は、この通過条件テーブルに基づいて、WANインターフェース部23で受信したパケットをLANインターフェース部25を介してLAN24側に転送するかを決定している。

図3Aにおいて、「送信元IPアドレス」の列は、WANインターフェース部23で受信したパケットの送信元IPアドレスを示し、「送信元ポート番号」の列は、WANインターフェース部23で受信したパケットの送信元ポート番号を示し、「宛先IPアドレス」の列は、WANインターフェース部23で受信したパケットの宛先IPアドレスを示し、「宛先ポート番号」の列は、WANインターフェース部23で受信したパケットの宛先ポート番号(ここでは、ポート番号に対応したプロトコル名により示している)を示し、「動作」の列は、WANインターフェース部23で受信したパケットの送信元情報と宛先情報が、通過条件テーブル28a中の送信元IPアドレス及びポート番号と宛先IPアドレス及びポート番号とそれぞれの値が一致した行に示される動作をそのパケットに対して行うことを示している。

【0009】

なお、「宛先ポート番号」の列で使用するプロトコル名とポート番号との対応は予め設定されている。また、「宛先ポート番号」の列には数値、つまりポート番号そのものを設定してもかまわない。

例えば、図3Aの通過条件の1行目では、送信元IPアドレス及びポート番号は「any(任意)」であり、これらIPアドレス及びポート番号に関係なく、宛先IPアドレスが「111.111.111.2」でかつ宛先ポート番号が「http(Hypertext Transport Protocol、例えばTCP(Transmission Control Protocol)の80)」であるパケットは、LAN14に転送される(通過: accept)。

【0010】

図3Aの通過条件の2行目では、送信元IPアドレスが「123.123.123.1」で、宛先IPアドレスの上位が「111.111.111」でかつ宛先ポート番号が「

h t t p s (hypertext transfer protocol security、例えば「h t t p s /」)である。パケットは、L A N 1 4 に転送され、3 行目では、送信元及び宛先の欄はいずれも「a n y」であり、「動作」の欄は「廃棄」であるから、全てのパケットが廃棄される(d r o p)。

アクセス制御部 2 6 中の検索部 2 6 a は、このような通過条件テーブル 2 8 a を上の行から、受信したパケットの送信先及び受信先情報が一致するか検証し、一致すれば指定された動作を転送制御部 2 6 b で行い、そのパケットに対する処理は終了する。この例では、図 3 A の通過条件テーブル 2 8 a に対し、上の行に設定された条件がより優先的に処理される条件となっている。

【0 0 1 1】

図 2 も参照してアクセス制御部 2 6 の動作を具体的に説明する。ファイアウォール装置 2 1 のアドレス宛の h t t p s の通過条件設定要求パケットを受信すると(ステップ S 1)、W A N 2 2 に接続された送信元の利用者端末 1 2 と安全なセッション、つまり S S L (Secure Socket Layer) セッションの確立をセッション確立・切断部 2 6 c で行い(ステップ S 2)、セッションが正常に確立されれば、セッション確立時に取得した送信元利用者端末 1 2 の I P アドレスを例えばデータベース部 2 8 に記憶し(ステップ S 3)、かつその認証情報要求を通信情報生成部 2 6 d の要求部 2 6 d 1 により利用者端末 1 2 へ送信する(ステップ S 4)。例えばユーザの識別情報とパスワードを入力させる H T M L フォームを暗号化して要求元利用者端末 1 2 に W A N インターフェース部 2 3 を介して送信する。この例では要求元利用者端末 1 2 の I P アドレスの他に、その条件設定要求パケット中に含まれる他の条件もデータベース部の通過条件テーブル 2 8 a に記憶する。

【0 0 1 2】

要求元利用者端末 1 2 から、暗号化されたユーザの識別情報とパスワードを受信すると(ステップ S 5)、この暗号化された認証情報を復号部 2 6 e により復号化を行い(ステップ S 6)、復号化されたユーザの識別情報とパスワードを認証処理部 2 7 に送信しユーザの認証を要求する(ステップ S 7)。

認証処理部 2 7 は、ユーザの識別情報とパスワードを受信すると、データベース部 2 8 中の認証情報部 2 8 b に蓄積してあるユーザの情報から、受信したユーザ識別情報と一致する識別情報を持つユーザを検索し、一致するユーザが見つかれば、認証情報部 2 8 b に蓄積してあるそのユーザのパスワードと受信したパスワードとを比較し、一致していれば、認証正常をアクセス制御部 2 6 に送信する。一致するユーザが見つからなかったり、パスワードが一致しなかった場合は、認証処理部 2 7 は認証異常をアクセス制御部 2 6 に送信する。

【0 0 1 3】

アクセス制御部 2 6 は、認証処理部 2 7 から認証正常(合格)を受信すると(ステップ S 8)、データベース部 2 8 の通過条件テーブル 2 8 a に蓄積されている。認証正常となったユーザの通過条件設定要求の情報に基づき、ステップ S 2 の S S L セッション確立時に取得した I P アドレスに対し、アクセスの許可、つまりパケット通過を設定する(ステップ S 9)。

例えば、認証正常となった I P アドレスが 1 2 3 . 1 2 3 . 1 1 1 . 1 の要求元利用者端末 1 2 に、I P アドレス 1 1 1 . 1 1 1 . 1 1 1 . 3 のサーバ(例えば L A N 2 4 に接続された W e b サーバ 1 6)の f t p (File Transfer Protocol)に対するアクセスを許可する(通過させる)場合、図 3 B に示すように、図 3 A に示した通過条件テーブル 2 8 a の一番上の行に、認証正常となった要求元利用者端末 1 2 に対する許可設定、つまりその要求元利用者端末 1 2 及び W e b サーバ 1 6 のアドレス情報と「動作」が「通過」の通過条件を追加する。一般の通過条件としては送信元アドレスは「a n y」でも良いが、この例では要求元利用者端末 1 2 の I P アドレスも設定される。

【0 0 1 4】

次に、アクセス制御部 2 6 は、認証が正常でアクセスが許可された旨と、アクセス可能情報(通過条件)としてアクセスが許可された例えば、W e b カメラなどのサービス名あ

るいは11ノドレへとポート番号、通信状況、ノドレへ制御部26dにおいて検出され、このIPアドレスが123.123.111.1の利用者端末から通信中となっている相手サーバ6のIPアドレス(111.111.111.3)とポート番号(ftp)などを表示するHTMLファイルを、通知情報生成部26dの許可部26d2及び状況部26d3により生成し、暗号化部26fで暗号化して要求元利用者端末に送信する(ステップS10)。

【0015】

利用者端末12では、このファイアウォール装置21から送信されたHTMLファイルを復号化して表示することにより、アクセス可能情報や、アクセス状況を表示することができる。

その後このようにして確立した利用者端末12とWebサーバ6とのSSLセッション中において、アクセス制御部26は、利用者端末12からのアクセスを監視部26gで監視し(ステップS11)、利用者端末12からのアクセスに異常を異常検出部26g1で検出すると(ステップS12)、その異常通知を通知情報生成部26dの異常部26d4で生成して、そのSSLセッションを通して利用者端末12へ送信する(ステップS13)。具体的には例えば以下の通りである。

(1) 利用者端末からのパケットの単位時間当たりのトラフィック(例えば、MB/sなど)は動画サービス、音声サービスなどサービスによってほぼ一定しているから、アクセス制御部26はSSLセッションが確立している端末からのパケットの単位時間当たりのトラフィックをサービス毎に監視し、サービス毎に予め設定されたトラフィック量を超えたトラフィックが発生したときは、そのサービス名や発生したトラフィック量などを表示するHTMLファイルを暗号化してその利用者端末に送信する。利用者端末12では、送信されたHTMLファイルを復号化して表示することにより、異常と思われるアクセスの情報が表示され、その利用者端末12の利用者は不正なアクセスがあることを知ることができる。

(2) 利用者端末12から、その利用者端末12に許可されていないサービスに対するアクセス要求があると、その数をサービス毎に計数しておき、その計数の値が予め設定された値、例えば1を超えたときは、そのサービス名や計数値などを表示するHTMLファイルを暗号化してその利用者端末に送信する。

【0016】

これを受信した利用者端末では、送信されたHTMLファイルを復号化して表示することにより、その利用者はその利用者端末と現にセッションを確立していない例えばWebサーバに対し、不正なアクセスがあったことを知ることができる。

(3) 同一の利用者端末からのファイアウォール装置21のアドレス宛のhttpsのアクセス要求パケット、つまり通過条件設定要求に基づくユーザの認証の異常の回数を計数しておき、その計数の値が予め設定された値を超えたときは、認証異常の回数が異常である旨とその計数値などを表示するHTMLファイルを暗号化してその利用者端末に送信する。

【0017】

これを受信した利用者端末では、送信されたHTMLファイルを復号化して表示することにより、正規の利用者はその表示のみで許可されていない利用者が前記正規の利用者になりすましてアクセスがあったことを知ることができる。

以上のようにしてアクセスを許可され、LAN24内のサーバ6との通信を行った利用者が、通信を終了するときは、ファイアウォール装置21から受信し、その利用者端末12にHTMLファイルで表示された画面から、通信の終了のボタンを選択するか、SSLセッションを切断する。

【0018】

ファイアウォール装置21のアクセス制御部26は、通信終了のパケットを受信したり、SSLセッションの切断を検出すると(ステップS14)、図3Bに示したように書き替えた通過条件テーブル28aを、図3Aに示したように元の状態に戻す。通信終了パケット受信の場合は通過条件テーブル28aを元の状態に戻すと共にそのSSLセッション

を切断する。ファイアウォール装置21のセッションの切断によるセッションの利用者端末の利用者に許可された通過条件を通過条件テーブル28aから直ちに削除し、その利用者に対するアクセス許可を解除する。

【0019】

ステップS14で通信が終了又はセッションが切断になっていなければステップS1に戻り、ステップS1で通過条件設定要求がなければ、ステップS11に飛びアクセス監視を行う。ステップS8で認証が合格しなければステップS16でセッション確立・切断部26cによりそのSSLセッションを切断してステップS1に飛ぶ。

なおステップS11、S12及びS13は通信状況監視ステップを構成している。また図1中において制御部27は各部を順次動作させたり、データベース部28に対する読み出し書き込み、消去などを行う。

【0020】

以上述べたように、この実施の形態においては、httpsのセッション内でユーザ（利用者）の認証を行い、認証が正常であればそのユーザに対応したアクセス許可（通過条件）をそのhttpsセッションを要求してきたIPアドレスに追加設定しているので、ファイアウォール装置21の外側からファイアウォール装置21のセキュリティポリシー（通過条件）をより安全に変更することができる。しかもセッションが切断されると、その追加設定した通過条件を直ちに削除するため、それだけ不正なアクセスを防止できる。

またこの実施形態では追加設定の通過条件に認証された通過条件設定要求元端末のIPアドレス情報が含まれているから、この点からも不正アクセスを防止できる。

【0021】

更にそのhttpsセッションにアクセスを許可したサービス名や、アクセスを許可したIPアドレスとの通信状況を表示しているので、これをユーザが確認することにより不正なアクセスを防ぐことができる。

また、ユーザの要求により、またはhttpsセッションの切断により、そのhttpsセッションを利用する通信が終了すれば直ちに変更したアクセス許可（通過条件）の設定状態を元に戻しているのでファイアウォール外からの変更した通過条件設定を利用しての不正アクセスを防ぐことができる。

【0022】

上述では利用者端末単位での通過条件設定要求に対して処理したが、ネットワーク単位での通過条件設定要求に対してもこの発明を適用できる。例えば図1中に破線で示すようにWAN22に例えば家庭内のホームネットワーク31が接続され、このホームネットワーク31に複数の利用者端末12が接続されている。この場合認証時にユーザの識別情報とパスワードとともにネットワーク単位での通過条件設定アクセス許可要求が送信され、ユーザのアクセス情報に基づき、ネットワーク単位でのアクセスを許可する設定がされる。つまり、アクセス制御部26は、SSLセッション確立時に取得したIPアドレスのネットワークアドレスに対し、アクセスの許可、つまり「動作」を「通過」にした通過条件を設定する。

【0023】

例えば、認証正常となったIPアドレスが123.123.111.0/24（上位24ビットが123.123.111、下位ビットが0, 1, 2, ..., 254のいずれか）の利用者端末、つまりネットワーク31に接続された利用者端末に、IPアドレス111.111.111.3のサーバ16のftp（File Transfer Protocol）に対するアクセスを許可する場合、図3Aに示した通過条件テーブル28aの一番上の行に、図4に示すように認証正常となった端末のネットワークアドレス（IPアドレスの上位24ビットが123.123.111であるIPアドレス）に対し許可設定、つまり「動作」を「通過」とした通過条件を追加する。

【0024】

また利用者端末とのSSLセッション確立中には、アクセス制御部26は、その利用者端末に対して、アクセス可能情報や、アクセス（通信）状況などを表示するHTMLファ

ールを唱へて返答する。

このようにすることにより、SSLセッションが確立中はネットワーク31内の利用者端末12のいずれからのアクセスでも許可することができ、しかもネットワーク31内のブラウザを持たない利用者端末からも許可された宛先に対しアクセスできるようになる。なお、通信状況はそのSSLセッション確立要求、つまり通過条件設定要求を行ったブラウザを持つ利用者端末へ送る。

【0025】

また、図2の利用者端末のIPアドレス又はネットワークアドレスに対し通過許可され、利用者端末とのSSLセッション確立中に、その利用者端末のIPアドレスが送信元IPアドレスに設定され、異なる宛先に対する接続要求のパケットを受信したとき、現に確立しているSSLセッションによりこの接続要求を許可するか否かをその利用者端末に問い合わせるようにしてもよい。

具体的には、ファイアウォール装置21とのSSLセッションが確立している利用者端末の利用者が、例えば現に受けているサービス以外のサービスを受けたい場合に、そのSSLセッションによりその通過条件設定要求を送信した場合は、現にSSLセッションが確立している利用者端末からその利用者端末のIPアドレスが送信元IPアドレスに設定された通過条件設定要求のパケットがアクセス制御部26に受信される。この受信によりアクセス制御部26は図2中のステップS1の次に破線で示すように追加設定処理S17を行う。つまりこの追加設定処理S17では例えば図5に示すように、受信した通過条件設定要求の要求元IPアドレスが、この要求が送信されたSSLセッションの利用者端末からであるか、つまり追加設定要求であるかを調べ（ステップS17a）、追加設定要求であれば、その利用者端末に対して、アクセス可能情報やアクセス状況などとともに追加設定要求のパケットを受信した旨と、その追加設定要求の宛先のIPアドレスおよびポート番号と、この追加設定要求を許可するか否かを選択させるボタンを表示するHTMLファイルを通知情報生成部26dで生成し、暗号化してそのSSLセッションにより利用者端末へ送信する（ステップS17b）。

【0026】

これを受信した利用者端末では、その送信されたHTMLファイルを復号化して表示することにより、追加設定要求が受信されたことがその利用者端末の利用者に通知され、かつその追加設定要求が利用者の想定したものであるかどうかをその利用者に確認させることができる。

要求に対する回答が受信され（ステップS17c）、アクセス制御部26でその回答をチェックし、その利用者端末から、その追加設定を許可する（追加通過条件設定を認める）であれば（ステップS17d）、アクセス制御部26は、その追加設定要求の通過条件を通過条件テーブル28aに追加設定する（ステップS17e）。

【0027】

従ってその後は現に確立してあるSSLセッションによりその追加通過条件を満たすパケットはLAN内の宛先のサーバに転送される。

ステップS17dで利用者端末からの回答が接続を拒否するのであれば、アクセス制御部26は、その新たな接続要求（追加設定要求）のパケットを廃棄する（ステップS17f）。このように確立されているSSLセッションを通じて追加設定要求が行なわれる場合に限らず、そのSSLセッションにより、例えばそのSSLセッションを確立する際に受けた通過条件設定要求と異なる例えばサービスを提供するサーバに対するサービス要求アクセスがなされる場合は、通常はその通過条件がデータベース部28に設定されていながら、ファイアウォール内への通過が許否されるが、このアクセスパケットに対し、アクセス制御部26は図5に示したように、ステップS17a、S17b、S17c及びS17dの処理が行われ、ステップS17dにおいて回答が許可するであれば、そのサービス要求パケットを対応するサーバへ転送する（ステップS17eの括弧書）ようにしてもよい。つまり確立したSSLセッションによる、要求元利用者端末のIPアドレスと同一の要求（送信）元IPアドレスが付加された追加条件設定要求や他宛先へのアクセス要求な

この接続要求に対して認証処理を行なうことができ、その結果セッションによる認証サーバへ転送させることができる。

【0028】

このように、新しい接続要求を許可するか否かをSSLセッションによりその利用者端末の利用者に問い合わせているので、不正なアクセスを防ぐことができる。

なお、この実施の形態においては、利用者端末からの安全なセッションとしてhttpsを用いたが、SSH (Secure Shell) などによる安全なセッションを使っても良い。ファイアウォール装置21に、図1に破線で示すようにサーバ16が直接接続されていてもよい。

上述では通過条件設定要求があれば、その要求元端末と安全なセッションを先ず確立し、その後認証処理を行ったが、先ず認証処理を行ってもよい。つまりステップS1で通過条件設定要求が受信されると図2中に破線で示すように直ちにステップS4に移り、認証処理を行い、その認証に合格すれば、ステップS9でデータベース部28にその通過条件を設定し、かつ要求元端末との間に安全なセッションを確立する。

【0029】

上述において認証処理部27をファイアウォール装置21内に設けたが外部に設けてもよく、つまり例えばLAN24に接続された認証サーバであってもよい。その場合はデータベース部28から認証情報部28bは省略される。更に認証処理としてはユーザ識別情報及びパスワードを要求し、これが認証情報部28b内に在るかないかで認証の合格か否かを決定したが、より安全度が高い認証方法を用いてもよい。

図1に示したファイアウォール装置をコンピュータにより機能させてもよい。この場合は例えば図2に示した各ステップをコンピュータに実行させるプログラムをコンピュータ内にCD-ROM、磁気ディスク、半導体記憶装置などの記録媒体からインストールし、又は通信回線を介してダウンロードして、そのコンピュータにそのプログラムを実行させればよい。

【図面の簡単な説明】

【0030】

【図1】 この発明の一実施形態におけるファイアウォール装置とこれが適用されたシステムの例を示すブロック図。

【図2】 この発明の一実施形態におけるファイアウォール方法の手順の例を示す流れ図。

【図3】 図1中の通過条件テーブル28aの記録例を示し、Aは新たな通過条件設定前、Bは新たな通過条件設定後の図である。

【図4】 ネットワーク単位のアクセスに対し通過条件を設定した通過条件テーブルの記録例を示す図。

【図5】 この発明の変形例処理手順の一部を示す流れ図。

【図6】 従来のファイアウォール装置を説明するためのシステム構成を示す図。

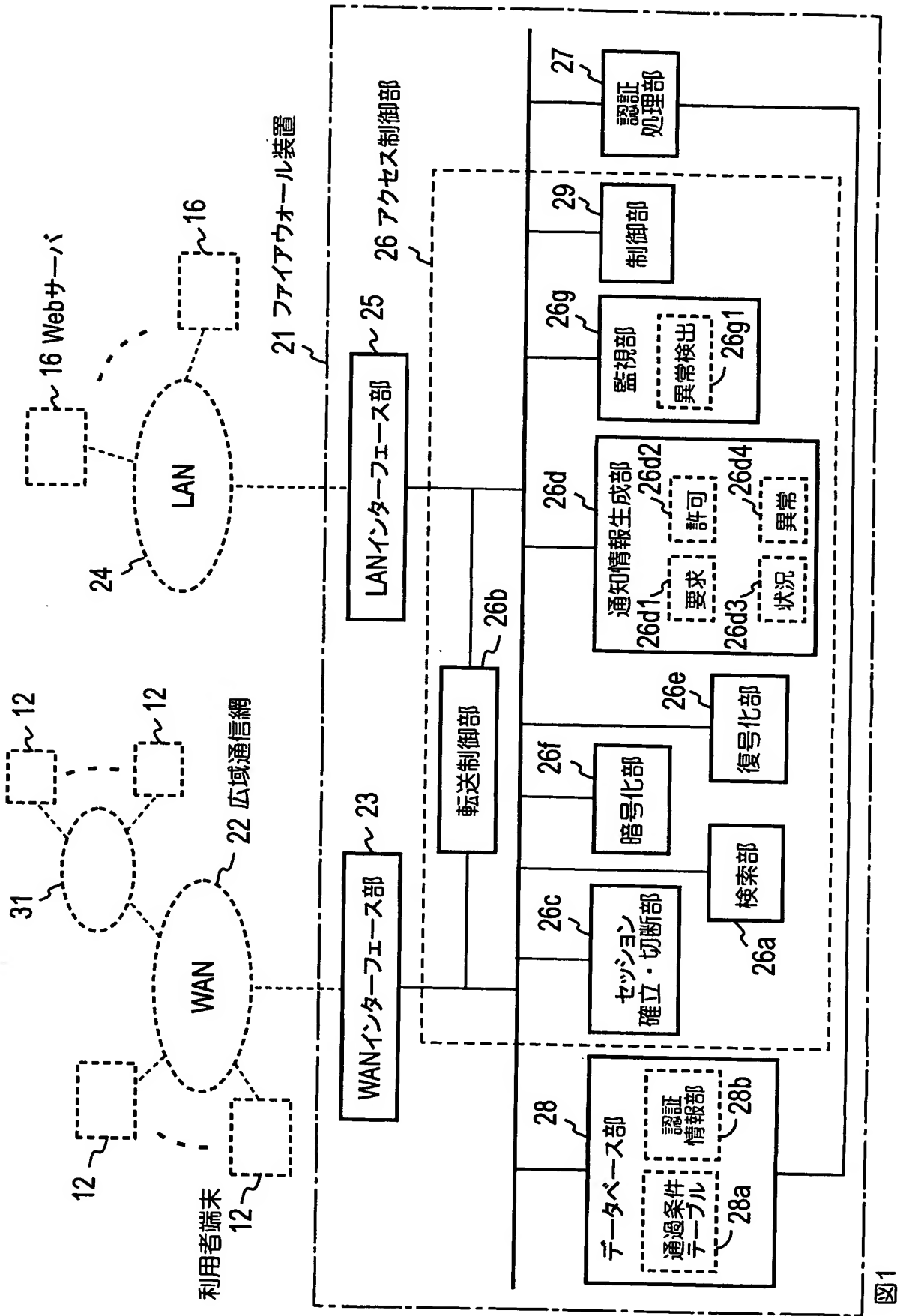


図1

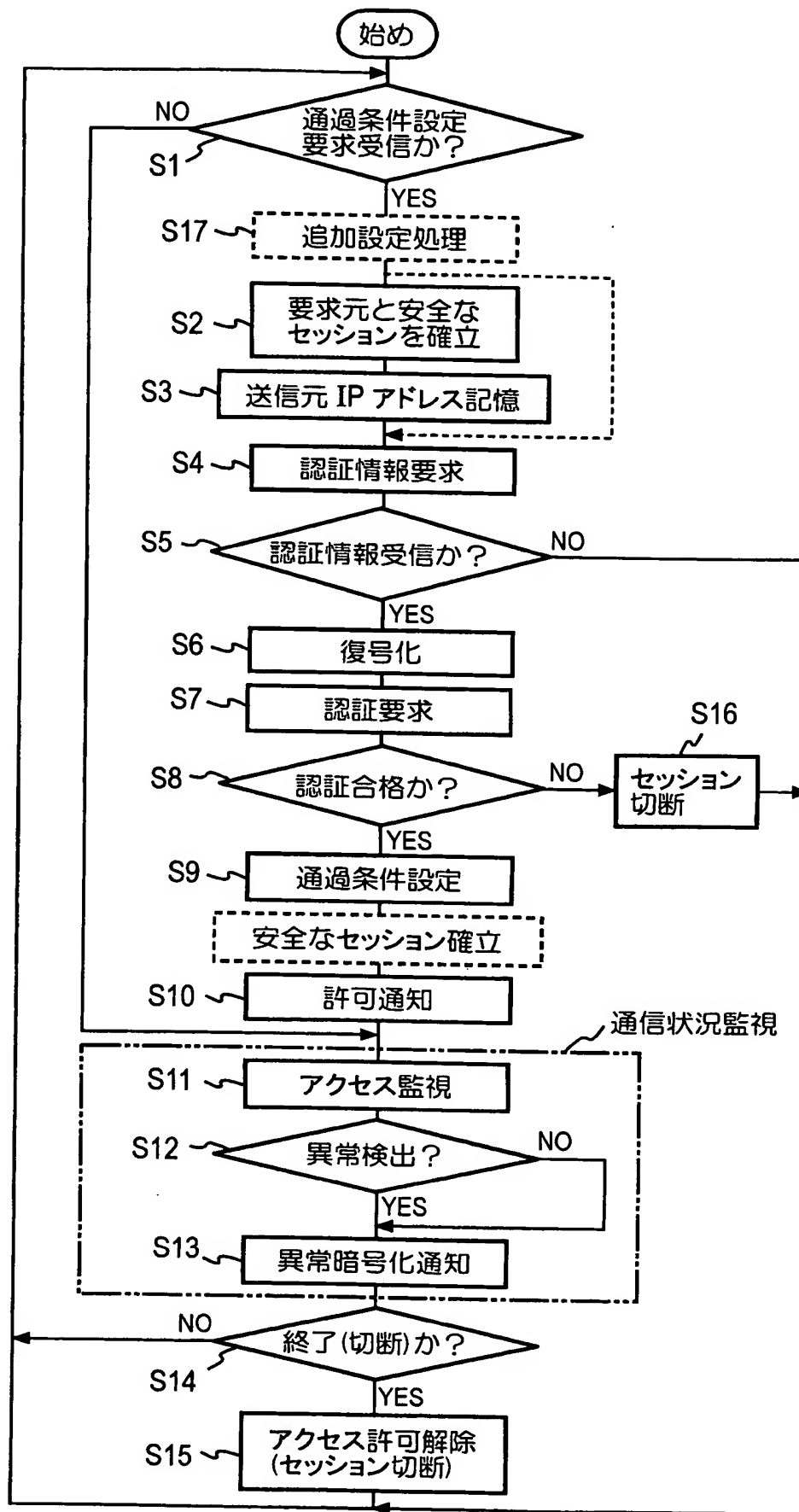


図2

送信元 IP アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	動 作
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.*	https(ssl)	通過
any	any	any	any	廃棄

A

送信元 IP アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	動 作
123.123.111.1	any	111.111.111.3	ftp	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.*	https(ssl)	通過
any	any	any	any	廃棄

B

送信元 IP アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	動作
123.123.111.0/24	any	111.111.111.3	ftp	通過
any	any	111.111.111.2	http	通過
123.123.123.1	any	111.111.111.*	https(ssl)	通過
any	any	any	any	廃棄

図4

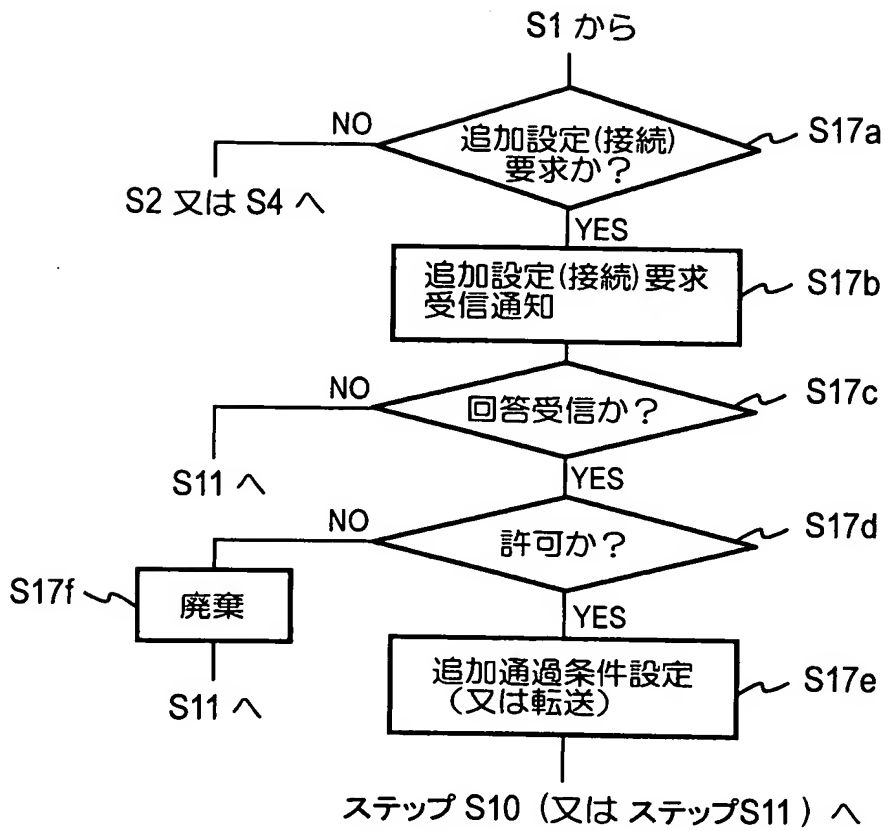


図5

【図 6】

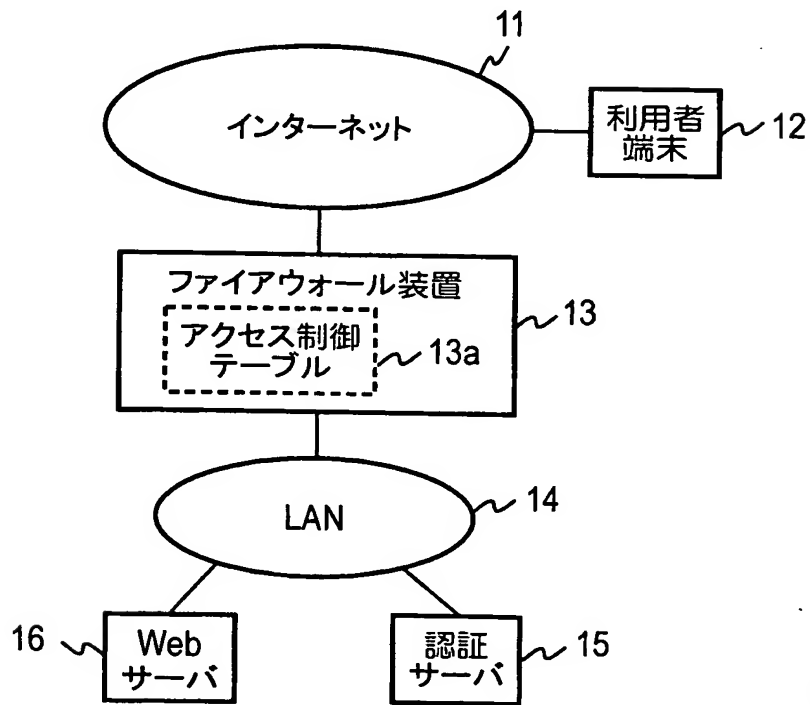


図6

【要約】

【課題】 セキュリティポリシーを動的に変えてもセキュリティを確保することができる。

【解決手段】 アクセス制御部26は、httpsのアクセス要求パケットを受信すると、送信元端末12のIPアドレスをデータベース部28に記憶すると共にhttpsセッションによりユーザの識別情報とパスワードを取得し、認証処理部27によりユーザの認証を行い、認証正常であれば、データベース部28に蓄積されている、端末のIPアドレスに対し、アクセス要求パケットに含まれている情報に基づき、アクセス許可を設定する。その後、前記httpsセッションによる例えばWebサーバ16に対するアクセス状況などをアクセス制御部26は、httpsセッションにより、送信元端末12へ送って表示する。また、アクセス制御部26は、通信終了のパケットを受信したり、httpsセッションの切断を検出すると送信元端末のIPアドレスに対するアクセス許可をデータベース部28から削除する。

【選択図】 図1

0 0 0 0 0 4 2 2 6

19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/007254

International filing date: 14 April 2005 (14.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-118740
Filing date: 14 April 2004 (14.04.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse